TEKPYME

TEKPYME

SECURITY AS A SERVICE

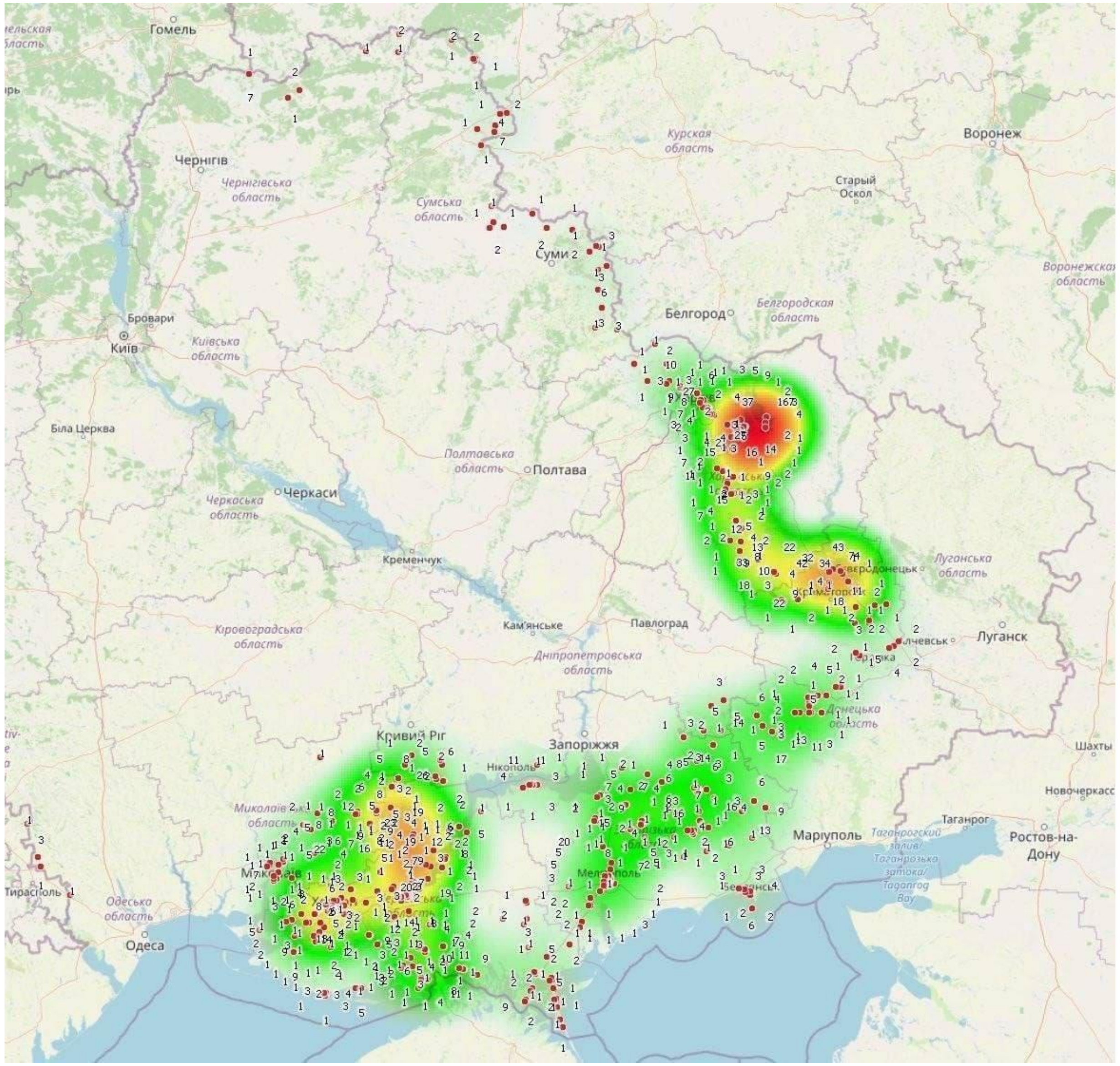
TEKPYME

Carlos Rubio Herrera

Area Manager Tekpyme

www.linkedin.com/in/carlos-rubio-herrera-54367942

☎ 621180523//mail:carlosrubio@tekpyme.com

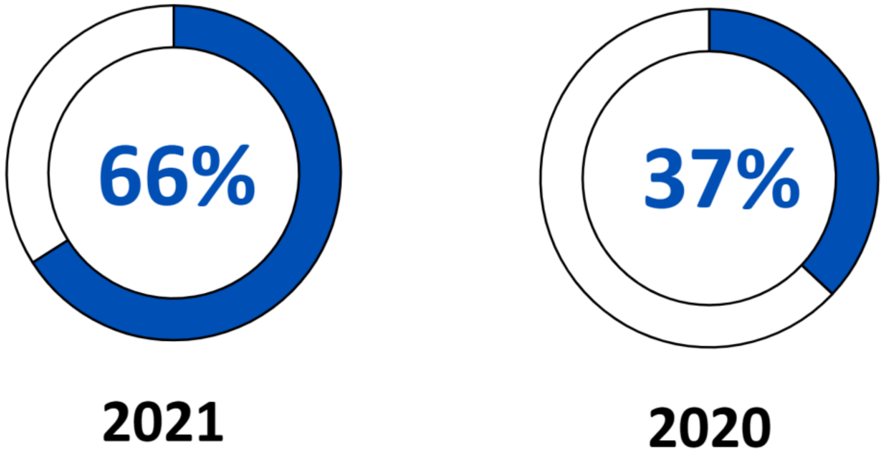


A heatmap of phones connected to the Russian mobile network in Ukraine shows an approximate representation of where Russian troop concentrations are in the country

TEKPYME

Ransomware Attacks Are Increasing

Hit by ransomware in the last year



Ransomware Recovery Is A Complex Process

1 MONTH
Average recovery time

SLOWEST	FASTEST
Higher Education Central/Federal Government	Manufacturing/ Production Financial Services

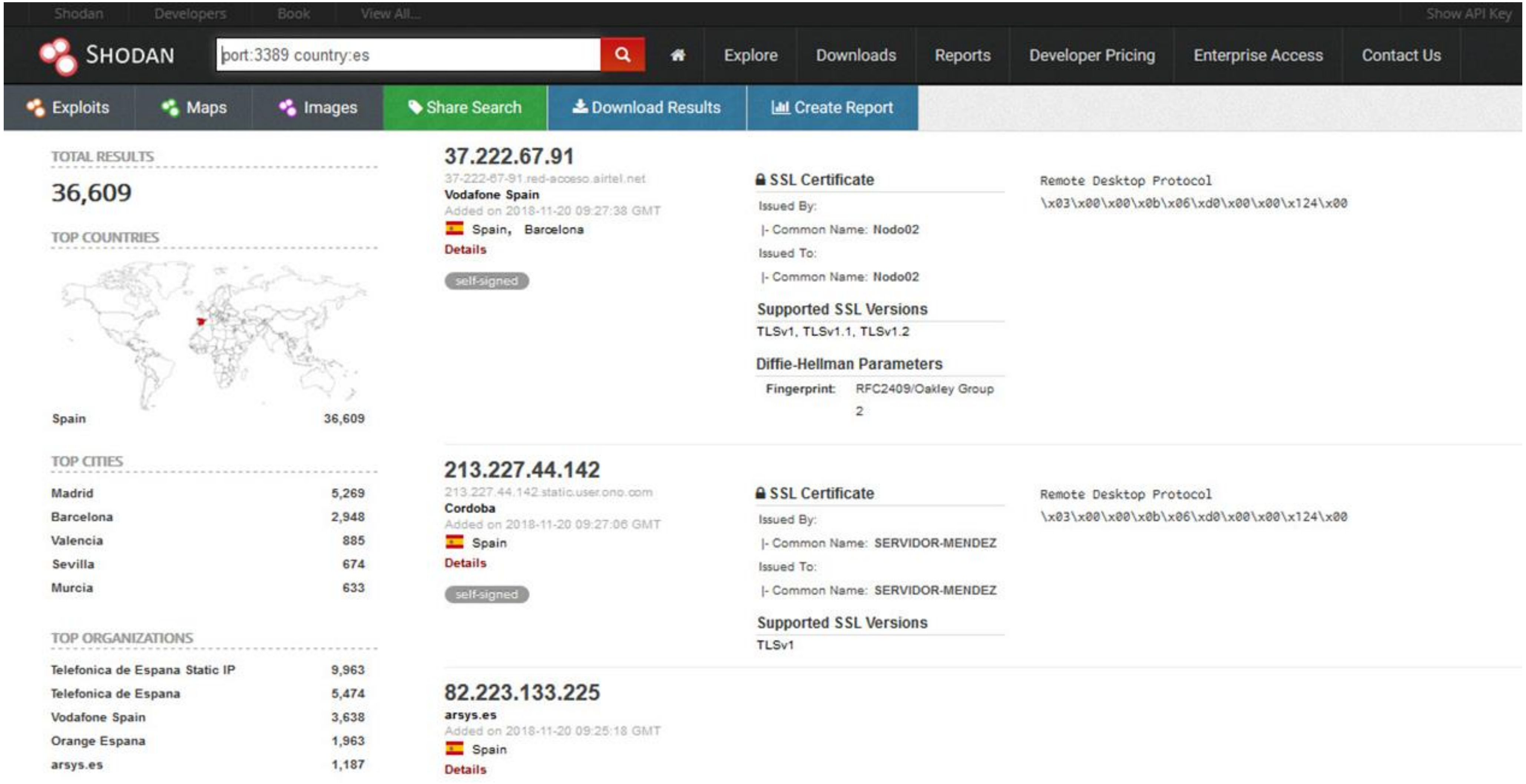
How long did it take your organization to fully recover from the most significant ransomware attack? (n=3,702 organizations that were hit by ransomware in the previous year)

Ransomware Remediation Is a Seven-digit Bill

US$1.4M	US$1.85M
2021	2020

What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.)? (2021 n=3,702/2020 n=2,006 organizations that were hit by ransomware in the previous year)

TEKPYME



TOTAL RESULTS

36,609

TOP COUNTRIES

Spain	36,609

TOP CITIES

Madrid	5,269
Barcelona	2,948
Valencia	885
Sevilla	674
Murcia	633

TOP ORGANIZATIONS

Telefonica de Espana Static IP	9,963
Telefonica de Espana	5,474
Vodafone Spain	3,638
Orange Espana	1,963
arsys.es	1,187

37.222.67.91

37-222-67-91.red-acceso.airtel.net

Vodafone Spain

Added on 2018-11-20 09:27:38 GMT

Spain, Barcelona

Details

self-signed

SSL Certificate

Issued By:

|- Common Name: Nodo02

Issued To:

|- Common Name: Nodo02

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

213.227.44.142

213.227.44.142.static.user.ono.com

Cordoba

Added on 2018-11-20 09:27:06 GMT

Spain

Details

self-signed

SSL Certificate

Issued By:

|- Common Name: SERVIDOR-MENDEZ

Issued To:

|- Common Name: SERVIDOR-MENDEZ

Supported SSL Versions

TLSv1

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

82.223.133.225

arsys.es

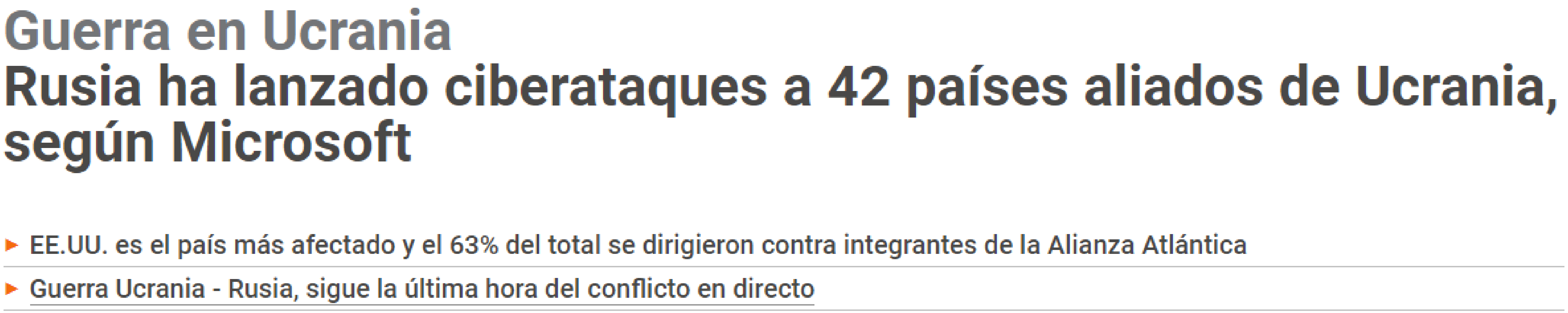
Added on 2018-11-20 09:25:18 GMT

Spain

Details

¿How can a company combat cyber attacks?

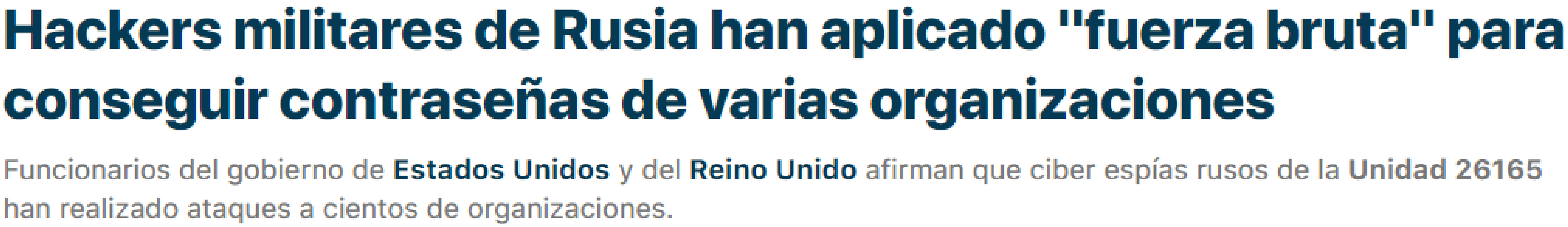
TEKPYME



Guerra en Ucrania

Rusia ha lanzado ciberataques a 42 países aliados de Ucrania, según Microsoft

- EE.UU. es el país más afectado y el 63% del total se dirigieron contra integrantes de la Alianza Atlántica
- Guerra Ucrania - Rusia, sigue la última hora del conflicto en directo



Hackers militares de Rusia han aplicado "fuerza bruta" para conseguir contraseñas de varias organizaciones

Funcionarios del gobierno de **Estados Unidos** y del **Reino Unido** afirman que ciber espías rusos de la **Unidad 26165** han realizado ataques a cientos de organizaciones.

Intercept attacks with preventive measures

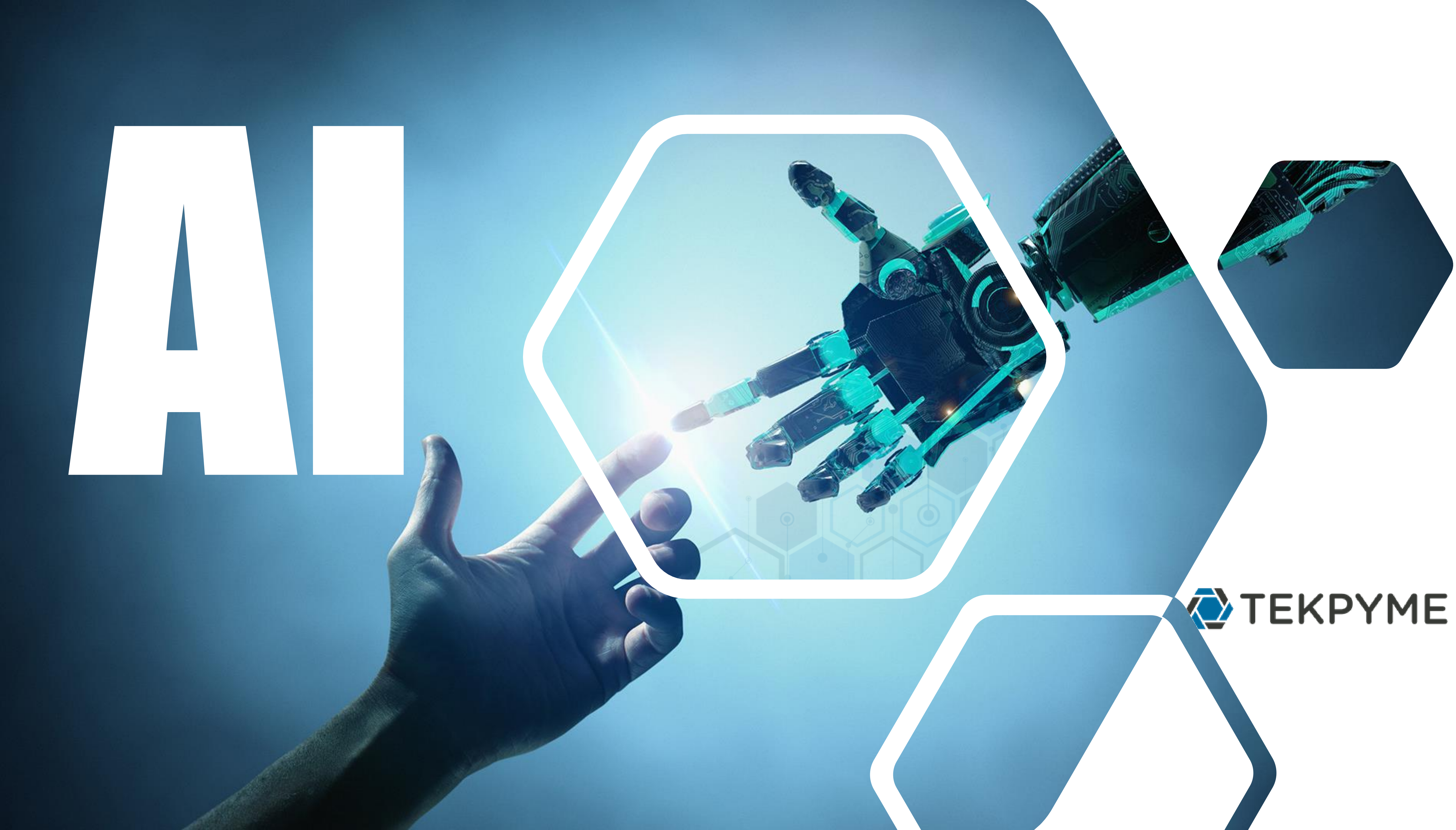
Brute force attacks

System administrators should ensure passwords are encrypted whith the highest rates possible

Users must choose 10 characters passwords, including numbers or symbols

TEKPYME

AI



TEKPYME

- Nowadays we can do a constant scanning of the operational network to detect intruders through programs based on artificial intelligence

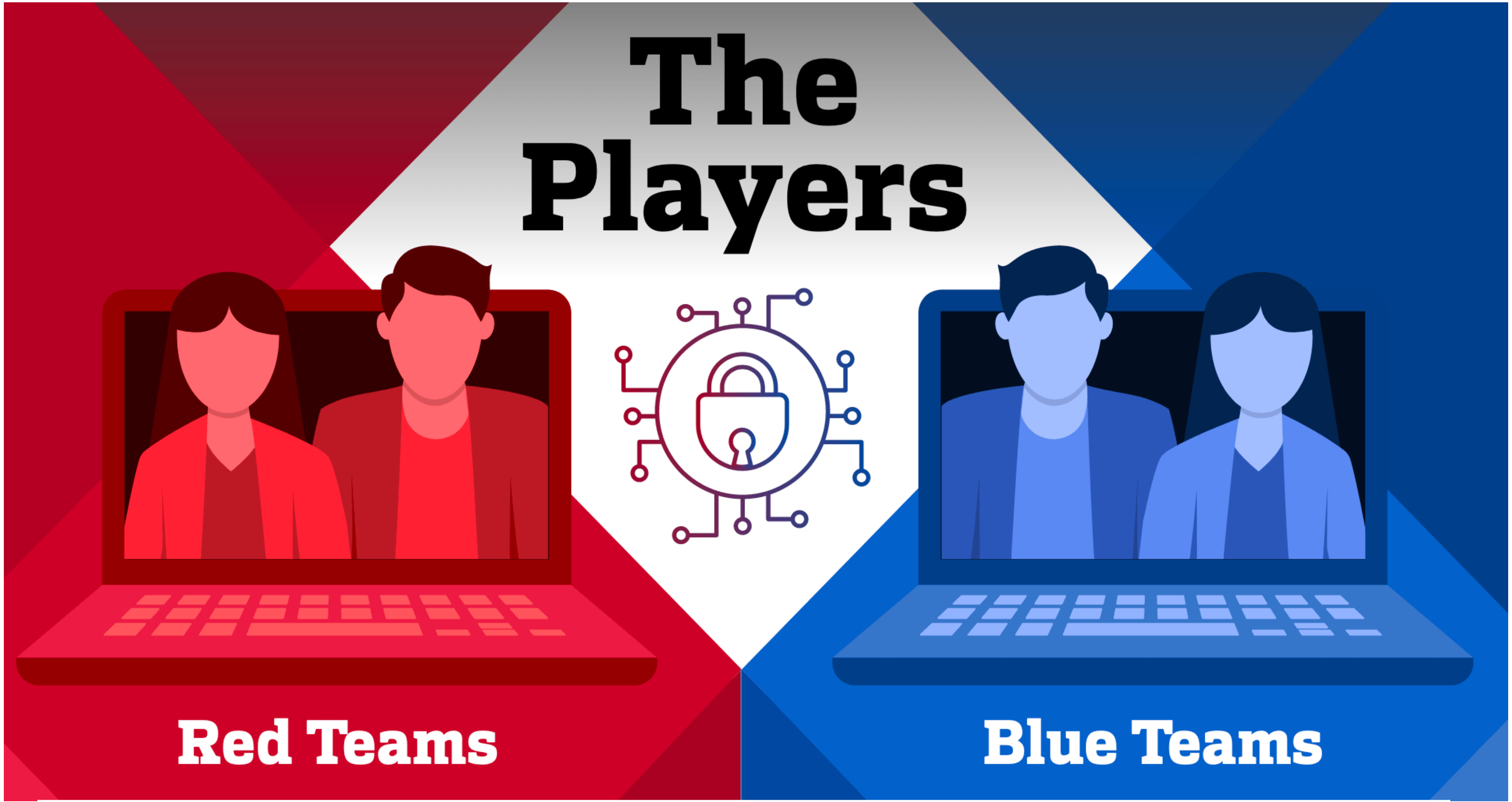
Threat Hunting

TEKPYME

Exercises and team training

TEKPYME

The Players



Red Teams

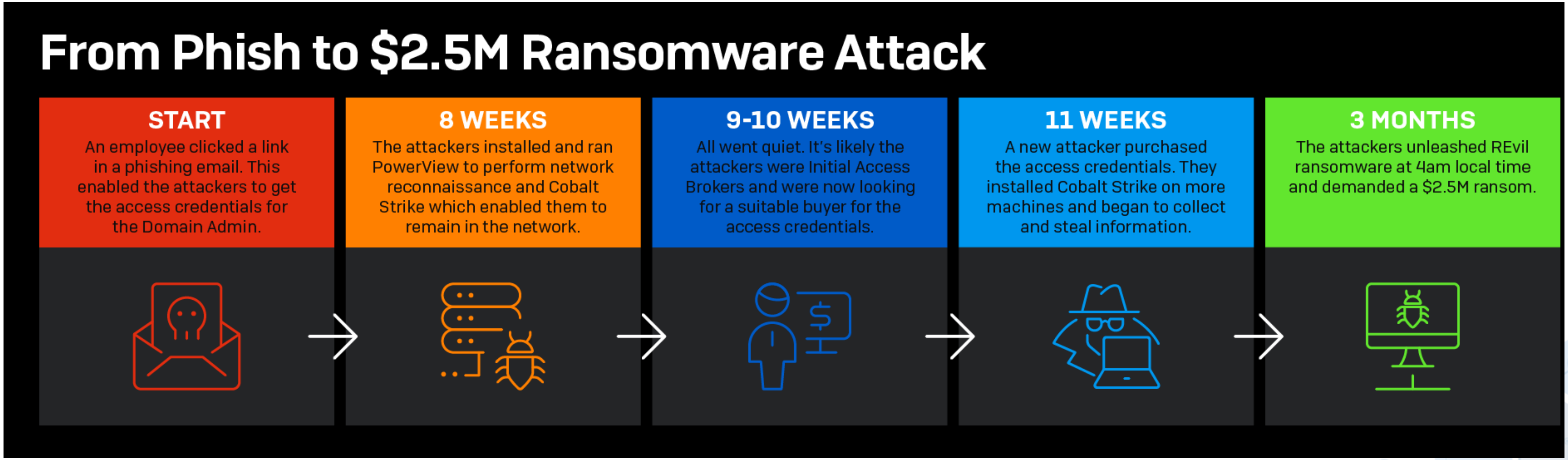
Blue Teams

PROACTIVITY	DEFENSE
DETECT CRITICAL POINTS	CREATE ACTION PLANS
MEASURE DETECTION&RESPONSE CAPACITY	ASSESS POTENTIAL THREATS
ASSESS DEGREE OF VULNERABILITY	ANALYSIS

TEKPYME

PHISING

Gamaredon would be behind a massive phishing campaing against Ukraine as revealed by an investigation carried out by Microsoft.



From Phish to $2.5M Ransomware Attack

START
An employee clicked a link in a phishing email. This enabled the attackers to get the access credentials for the Domain Admin.

→

8 WEEKS
The attackers installed and ran PowerView to perform network reconnaissance and Cobalt Strike which enabled them to remain in the network.

→

9-10 WEEKS
All went quiet. It's likely the attackers were Initial Access Brokers and were now looking for a suitable buyer for the access credentials.

→

11 WEEKS
A new attacker purchased the access credentials. They installed Cobalt Strike on more machines and began to collect and steal information.

→

3 MONTHS
The attackers unleashed REvil ransomware at 4am local time and demanded a $2.5M ransom.

TEKPYME

The most common cyber attack on any organization

There are some programs or platforms that can simulate Phish attacks to see how the teamworks response

Every user in every organization need to be trained on phising

Organizations should analize the protection they have against a phishing attack

TEKPYME

IT department

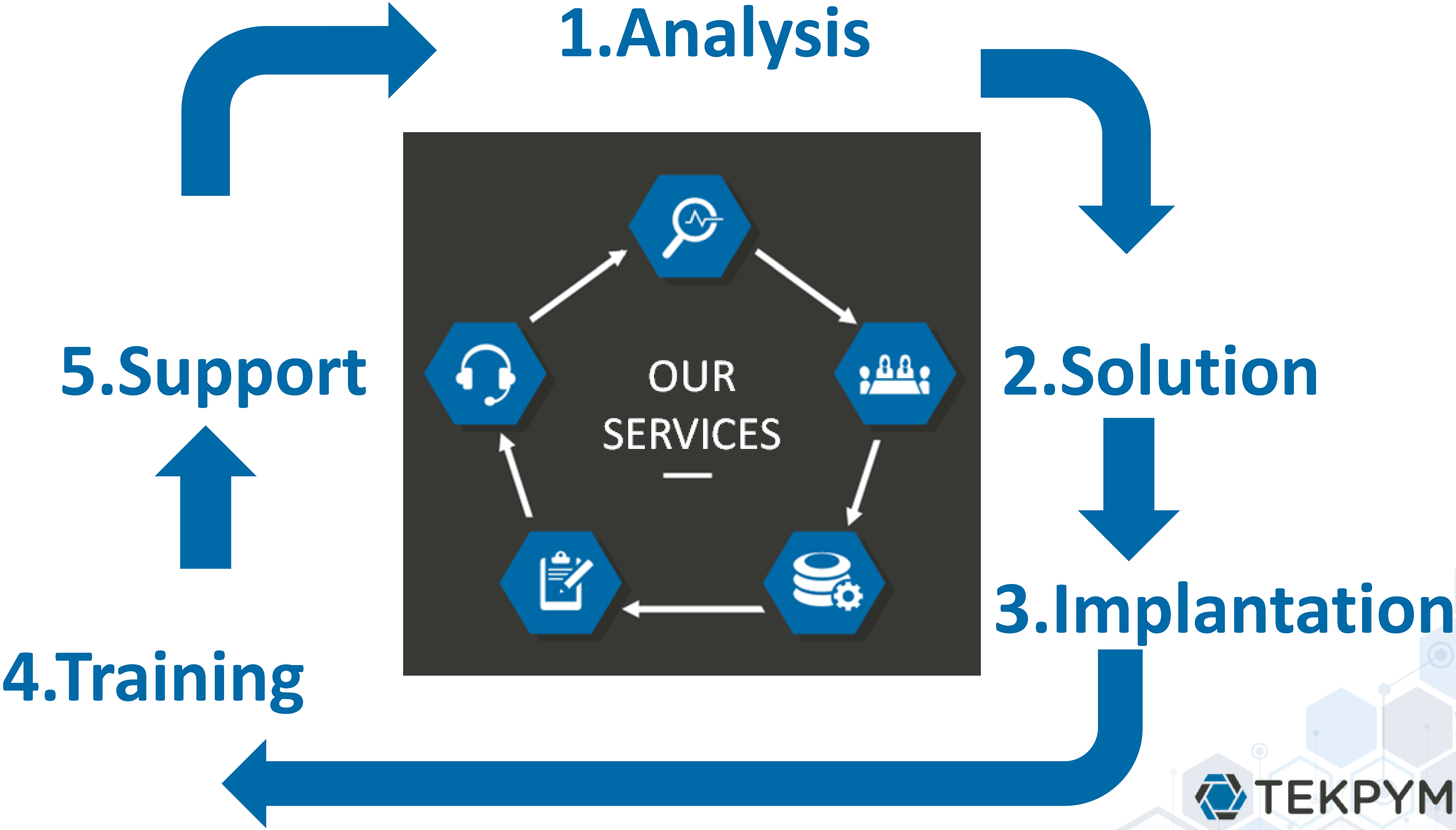
The biggest challenge for an IT department is keeping up with digital transformation and retaining technical talent

TEKPYME

WHAT WE OFFER TO OUR COSTUMERS ?

- Outsource the IT department
- Offer an integrated solution to each type of company
- Offer the management of the entire infrastructure of each company or organization
- Provide 24/7 solutions to all incidents
- Be in continuous training
- Specialization

TEKPYME



1.Analysis

2.Solution

3.Implantation

4.Training

5.Support

TEKPYME

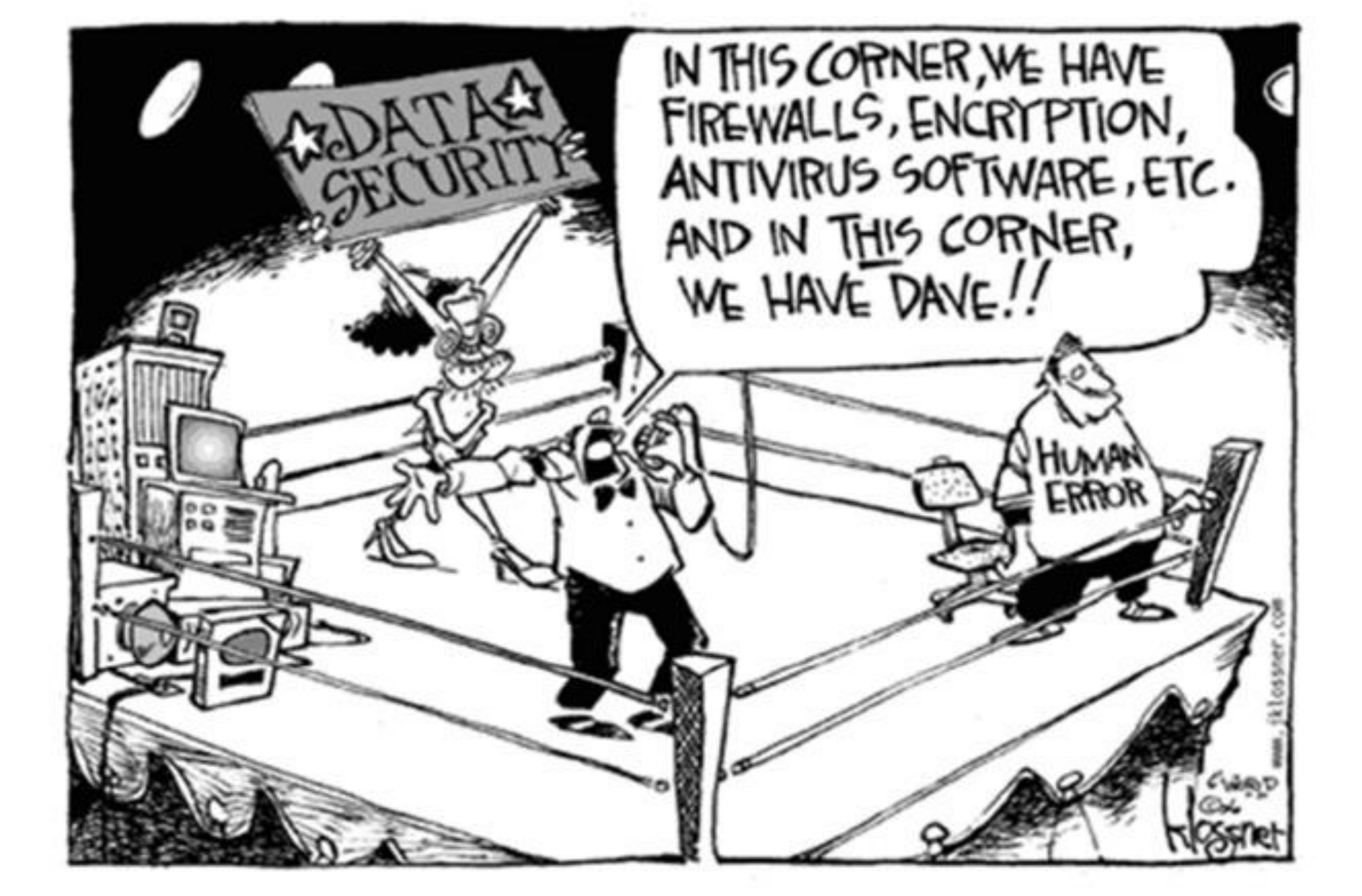
Summary

- All the organizations have to be analyzed
- There are only 2 tipes of cybersecurity hacked or not hacked
- If something is connected to the network it must be protected

TEKPYME

THANK YOU

TEKPYME


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©WORD 06
Klossner

TEKPYME

Carlos Rubio Herrera

Area Manager Tekpyme

www.linkedin.com/in/carlos-rubio-herrera-54367942

☎ 621180523//mail:carlosrubio@tekpyme.com